Science and Technology: A Foundation for Homeland Security

Office of Science and Technology Policy

April 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Science and Technology: A Foundation for Homeland Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Eexecutive Office of the President Office of Science and Technology Policy Washington, D.C. 20502**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**60**	

Science and Technology:
A Foundation for Homeland Security

Office of Science and Technology Policy

April 2005

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

Dear Colleague,

Our Nation has made significant strides to protect the homeland since the terrorist attacks of September 11, 2001. Since those tragic events, more than 1,000 days ago, the Federal government has responded in numerous ways to protect against future attacks. Science and technology have played a vital part in the progress made to date, and will continue to inform and enhance our country's homeland security effort.

Science and Technology: A Foundation for Homeland Security details the numerous accomplishments of science and technology that have helped to secure the homeland. This document builds upon the National Strategy for Homeland Security, released by the President on July 16, 2002, which set forth a sound framework to reduce America's vulnerability and to respond with improved agility and effectiveness to future terrorist attacks.

Some key accomplishments highlighted in the document include:

- Bolstering border security through the development and deployment of nuclear detection equipment along the U.S. border, airports, and seaports to detect, deter, and ultimately prevent the trafficking of nuclear and radioactive materials.
- Providing an early warning system for bio-threats through Project BioWatch, a cooperative effort among the Department of Homeland Security, the Environmental Protection Agency, and the Centers for Disease Control and Prevention Laboratory Response Network.
- Speeding development and procurement of new medical countermeasures against current and future chemical, biological, radiological, and nuclear terrorist threats through Project BioShield, an initiative signed into law by the President in July 2004.

These scientific and technological accomplishments represent only a small portion of our Nation's broad and intense effort to combat terrorism. There will always be more to do, as the terrorist threat we face is constantly evolving, but I know we are now better prepared to defend ourselves against this threat. Science and technology provide the foundation that enables the significant advances we have achieved.

Sincerely,

John H. Marburger, III
Director

Science and Technology: A Foundation for Homeland Security

Table of Contents

Science and Technology: A Foundation for Homeland Security

"We refuse to remain idle while modern technology might be turned against us; we will rally the great promise of American science and innovation to confront the greatest danger of our time." President George W. Bush, July 21, 2004

I. Introduction

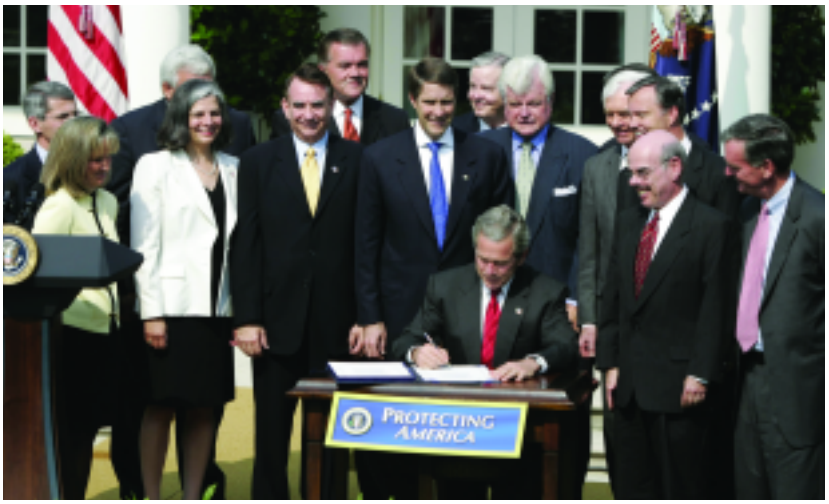
Three years have elapsed since the terrorist attacks of September 2001 and the subsequent anthrax attacks of October 2001. The Administration's response to these horrific events included calling on the full scientific and technical strength of the Nation to inform and enhance our country's homeland security effort.

On July 16, 2002, the President released the *National Strategy for Homeland Security* (herein referred to as the *National Strategy*), a visionary strategy that laid out a framework prompting bold and innovative steps to enhance our national protection and reduce America's vulnerability to terrorist attacks.

Since that time, much has been accomplished, and still more has been initiated.

The first section of this report outlines the numerous ways our country is more secure as a result of the application of science and technology (S&T) for homeland security as outlined in the *National Strategy*.

In the remaining sections, the details of accomplishments and on-going activities are provided, first concerning defense against catastrophic threats arising from chemical, biological, radiological, or nuclear weapons, and in the following section focusing on the remaining priority S&T initiatives. Although by no means exhaustive, these examples typify the progress that has been made in the key research areas designated as priority goals by this Administration in the *National Strategy*.



President George W. Bush signs S.15, the Project BioShield Act of 2004 in the Rose Garden, July 21, 2004. Ceremony Participants include, front row from left, Frances "Fran" Townsend, Dr. Julie Gerberding, Sec. Tommy Thompson, Sen. Bill Frist, Sen. Ted Kennedy, Sen. Thad Cochran, Rep. Chris Cox, Rep. Henry Waxman, Sen. Judd Gregg. 2nd row from left, Dr. Anthony Fauci, House Speaker Dennis Hastert, Sec. Tom Ridge, Rep. Joe Barton. White House photo by Paul Morse

II. How Do Science and Technology Help Keep Us Safe?

The Federal government has joined with academia, industry, and the national laboratories to apply the best talents and skills to make us less vulnerable and to improve our ability to prevent an attack or respond and recover if an attack should occur. While the focus is on reducing the threat from terrorism, much of the investment also serves to better prepare individuals and local governments to respond to and recover from naturally occurring disasters. As stated in the National Strategy, "The technologies developed through this research and development will not only make us safer, but also make our daily lives better; while protecting against the rare event, they should also enhance the commonplace."

But what new capabilities do we actually have? The examples given below illustrate the real-world impact of recent investments in science and technology for homeland security:

- On September 11, 2001, nineteen hijackers took control of four airplanes and murdered almost 3,000 innocent people. Of these nineteen hijackers, the 9-11 Commission staff noted that three carried passports with indicators of Islamic extremism linked to al Qaeda; two carried passports manipulated in a fraudulent manner; two lied on their visa applications; two hijackers violated terms of their visas; and three of the hijackers used fraudulently obtained state issued identifications to check in for their flights on September 11. Since September 11, the Government has invested to combine databases, terrorist watch lists, and centralizing other forms of information so that the relevant agencies will have the best information available to protect the Nation. In addition, the Government has developed and is deploying biometrics technologies to reliably confirm the identity of the individual. With the use of advanced biometrics and other data, it will be harder for someone wanting to do us harm to enter the United States.

- In times of crisis, the local emergency responders are usually the first on the scene. These are the local fire fighters, police, and emergency medical teams that are our neighbors, relatives, and friends. When they enter a hazardous area – they rely on their equipment to prevent exposure to hazards and communication gear to connect them to each other and their command. But officials must know that their equipment can be successfully used against the threats we face, including biological, chemical, and radiological substances. The United States Government is committed to ensuring the safety and security of emergency responders and is actively developing technologies for enhancing safety and promoting performance standards that manufacturers must meet. In addition, the Government is establishing training standards and programs, including operating a mock hospital facility dedicated to medical training in disaster preparedness and response for hospital and healthcare professionals.

- Just a few years ago, the only way that the public health community could identify the extent of a disease outbreak was through the intensive detective work of local public health officials working with the Centers for Disease Control and Prevention (CDC). These measures came into play only after a significant number of patients became ill and sought medical attention. In the past two years, the Federal government has installed sensors in major urban settings to detect the presence of biological or viral pathogens — before people become ill. Coupling detection with atmospheric models to predict where the

pathogens might disperse, the public health community can now identify potentially exposed populations and provide early treatment to prevent or minimize the onset of symptoms. In the near future this system will be expanded and, in combination with the tracking of other relevant information (such as notable increases in the sale of certain over–the-counter medicines), further refine our ability to detect and assess the impact of a bioterrorist attack.

- Members of the Aum Shinrikyo cult in Japan released sarin, a deadly nerve agent, into the Tokyo subway system in 1995. Within minutes, a dozen people were killed and thousands more were injured. To minimize the consequences if a similar attack occurs within the United States, an automated, early warning system for this country's subways has been developed and is now being tested in several cities.

- The outbreak of Foot and Mouth Disease in the United Kingdom (U.K.) during the summer of 2001 resulted in the death of millions of cattle, sheep, and pigs and cost the U.K. almost $5 billion. The U.S. Government learned many lessons from the U.K. experience. To address the threat of an intentional attack or a naturally occurring outbreak, the Administration established research initiatives to more rapidly diagnose animal illnesses and accelerate development of new animal vaccines. This research will enable the animal health community to respond more quickly to disease outbreaks, preventing the death of many animals and preserving the livelihood of the 15 percent of the U.S. population employed in agriculture or agriculture-related fields.

These examples illustrate some of the ways the Nation's significant investment in science and technology for homeland security has been returned to the public in improved technical capabilities that translate into increased security. While we have made much progress since the attacks of September 11, 2001, it is imperative that we continue to push the envelope of science and technology to provide the strongest possible foundation for the Nation's homeland security.

III. Science and Technology for Defense against Catastrophic Threats

Technological expertise to produce chemical, biological, radiological, and nuclear [1] (CBRN) weapons is proliferating. To counter this serious threat, the President established in December 2002 a National Strategy to Combat Weapons of Mass Destruction that calls for a coordinated national effort to prepare for, prevent, and respond to these threats to our homeland. The United States leads the world in science and technology capabilities, and we are committed to fully utilizing this national expertise in our continuing efforts to guard against catastrophic threats.

New research and the development of technologies form the foundation for programs to prevent such weapons from entering the country, for reducing our vulnerability to such weapons, and for recovering from an attack if one should occur. In addition, science and technology are being used to set the standards and guidelines that ensure that local and Federal responders can safely address any issues that arise.

A) Radiological and Nuclear Countermeasures [2]

The 2002 **National Strategy** *states: "Our highest scientific priority must be preventing terrorist use of nuclear weapons." Prevention is key. Tremendous benefit has already been realized through harnessing existing investments in the Nation's nuclear expertise to deter, defend against, and defeat potential attacks. An important element of deterring nuclear threats is control over fissile materials. The United States, through the efforts of the Departments of Energy, Defense and State, has made significant progress in ensuring nuclear security by improving our ability to safeguard and physically protect nuclear materials at target sites worldwide, including the states of the former Soviet Union, and over 40 countries holding nuclear material used for power and research reactors.*

"Our highest scientific priority must be preventing terrorist use of nuclear weapons."

2002 National Strategy

- We are bolstering border security through the development and deployment of nuclear detection equipment along the U.S. border, airports, and seaports to detect, deter, and ultimately prevent the trafficking of nuclear and radioactive materials.

- The Department of Homeland Security (DHS) is continuing to evaluate systems at U.S. ports-of-entry and at critical points in the transportation system. An example of this is the radiation testbed project established by DHS and the Port Authority of New York and New Jersey. This project involves the testing and assessment of candidate radiation detection systems for air, sea, or land. The project has successfully tested commercially available cargo radiation monitors, hand-held instruments that can distinguish commercial radioactive materials from those that

[1] Radiological weapons are those intended to disperse radioactive contamination, nuclear weapons involve fissile materials, and therefore result in nuclear explosion.

[2] Radiological and nuclear countermeasures include: controlling the availability of nuclear or radiological material, detecting and defeating threats, medical responses, and identifying and addressing radioactive contamination resulting from an attack.

constitute a threat and prototypes of the next generation of detection systems.

- The Department of Defense (DoD), through the **Unconventional Nuclear Warfare Defense** program in the Defense Threat Reduction Agency (DTRA), has developed and evaluated a range of technologies suited to the protection of military installations. The DoD **"Guardian" Installation Protection Program** will draw from this expertise in serving a larger mission: providing an integrated CBRN protection capability at 200 DoD installations and facilities worldwide.

- The Department of Energy (DOE) sponsors research in the development and manufacture of large, high-quality crystals of advanced materials used in radiation detection systems. Researchers from DOE, the academic community, industrial partners, and DoD are collaborating on a next-generation radiation detection system that will detect and identify radioactive materials to meet a wide variety of civilian and defense requirements.

- Several agencies (including DHS, the Department of Commerce's National Oceanic and Atmospheric Administration (NOAA), DoD and DOE) participate in the development of models to predict the dispersion and behavior of radioactive particles in the atmosphere following nuclear/radiological incidents.

- Ensuring that an individual or organization that attempts to target the United States with a nuclear weapon can be identified and brought to justice is a powerful deterrent to those who want to do us harm. The DoD and DHS have established programs to enhance our ability to identify the origin of materials and expertise used to develop such a weapon.

[3] www.tswg.gov/tswg/home/home.htm

- DoD, DHS, DOE, and the Environmental Protection Agency (EPA) are investing in methods for the detection, decontamination, and controlled clean-up of radioactively contaminated buildings and critical infrastructure to reduce the economic and psychological impacts of the dispersal of radioactive contamination. Through the introduction of novel methods to find and remove contamination (tailored to the building materials found in urban environments), it will be possible to avoid costly demolition in affected areas.

- With support from the Technical Support Working Group (TSWG) [3], an interagency group that funds application of promising new technologies, we have a number of practical tools for emergency responders. These include software tools to manage and assess casualties from radiation exposure.

- The DoD's Armed Forces Radiobiology Research Institute (AFRRI) has made significant progress in identifying medical countermeasures to the effects of ionizing radiation, which can harm living tissues. Scientists at AFRRI are currently developing radioprotectants (substances that protects against the radiation's effects either by preventing injury or promoting healing) that stimulates the production of infection-fighting white blood cells in subjects exposed to whole-body ionizing radiation, such as could occur in the aftermath of a nuclear attack.

B) Biological and Chemical Threat Agent Detection

Early detection of a chemical or biological attack is critical for an effective public health response. Early detection enables a critical link to be made between an outbreak and the systems that will help minimize injury and death.

President Bush issued two Homeland Security Presidential Directives (HSPD-9 and 10) that call for increased research and development to defend against biological threats to our people, economy, agriculture, food, and water supplies. HSPD-9 establishes a national policy to provide protection against an attack on the agriculture and food systems. HSPD-10/National Security Presidential Directive-33, *"Biodefense for the 21st Century,"* builds on our past accomplishments, specifies roles and responsibilities, and integrates the national security, public health, and law enforcement efforts into a sustained and focused national program to guard against the use of biological threat agents.

The President's **Biosurveillance Initiative**, is a government-wide effort to protect the American public from possible bioterror attacks. The Biosurveillance Initiative integrates real-time information on the health of the Nation's human and agricultural (plant and animal) populations with environmental monitoring of air, food (domestic and imported, including animal feed), water, and threat intelligence data. Key elements of the Biosurveillance Initiative include:

- **National Biosurveillance Integration System (NBIS)** — DHS is developing a system to integrate data collected from sensors throughout the country and will fuse this data with information from health and agricultural surveillance and with other terrorist-threat information from the law enforcement and intelligence communities.

- **Project BioWatch** involves cooperation among DHS, EPA, and the CDC **Laboratory Response Network**[4] to provide an early warning system for bio-threats. Since 2003, Project BioWatch has monitored atmospheric samples in more than 30 U.S. cities around-the-clock. With the quick detection of biological threat agents, life-saving therapies can quickly be distributed to citizens in affected areas.

- **Project BioSense** — CDC initiated an effort in Fiscal Year (FY) 2003 to enhance our ability to monitor human health events. The BioSense system, which operates nationwide, allows the CDC and state and local health departments to monitor the health status of populations by analyzing diagnoses at ambulatory care sites, in laboratory testing orders, in over-the-counter drug sales, and other select data sources. It can integrate these human health surveillance disease trends with the environmental sampling from Project BioWatch to present a coordinated view for public health response management.

Other Federal efforts to develop early warning systems to detect, characterize, and eliminate possible biological or chemical materials and attacks include:

- DHS, in collaboration with local governments, has developed a chemical agent detection and response system for urban mass transit systems. This system has been deployed in a number of transit stations and provides near real time

[4] The Laboratory Response Network (www.bt.cdc.gov/lrn/factsheet.asp) is a network of State/government public health labs that provide surge capacity for samples testing during a public health emergency caused by biological and chemical terrorism.

analysis of possible chemical agents and communicates that information to emergency responders to facilitate response and recovery. This system also has application in supporting emergency response to naturally occurring events such as fires and in assisting station managers with routine security operations.

- DoD's Walter Reed Army Institute of Research (WRAIR) oversees the identification of possible biological threats to populations world-wide through the **Global Emerging Infections System (GEIS)** and the **Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE)**.

- EPA has tested and evaluated technologies for detecting contaminants in drinking water, disinfecting contaminated water, and decontaminating equipment and infrastructure through its **Environmental Technology Verification Program (ETV)**.

c) Medical Countermeasures [5]

The Administration is aggressively pursuing the development and acquisition of medical countermeasures to safeguard U.S. citizens against possible attacks using weapons of mass destruction (WMD). Under the President's direction, a comprehensive, end-to-end review of the Nation's biodefense capabilities culminated in the ***National Strategy for Biodefense in the 21st Century****.* [6] *This Presidential directive charted a course for the future that, among other things, will ensure the Nation fully leverages the scientific capabilities that exist both inside and outside the Federal government in the development of countermeasures against attacks using CBRN threat agents.*

In July 2004, the President signed into law **Project BioShield**, which will speed development and procurement of new medical countermeasures against current and future CBRN terrorist threats. The President has committed $5.6 billion over ten years for the Government to accelerate development and stockpile vaccines, drugs, and diagnostic aides to fight anthrax, smallpox, and other potential CBRN threat agents.

Through the BioShield program, the President has strengthened the **Strategic National Stockpile** (SNS).[7] The SNS consists of drugs, vaccines and medical equipment, stored at multiple sites throughout the United States, which can be quickly dispersed to affected communities during a public health emergency. Already the SNS includes enough smallpox vaccine for every American, and the Department of Health and Human Services (HHS) is using BioShield appropriations to acquire 75 million doses of the next generation anthrax vaccine. Under BioShield, the Government also has contracted to acquire the improved smallpox vaccine, better treatment options for anthrax infection, and countermeasures to botulinum toxin, among other priorities.

Specific Federal agency programs in biodefense research and development of medical countermeasures include:

[5] Medical countermeasures include **vaccines** to prevent illness from exposure to a terrorism agent; **diagnostic tools** to identify whether a patient has been exposed to a terrorism agent; and **drugs** to treat illness resulting from exposure to a terrorism agent.
[6] www.whitehouse.gov/homeland/20040430.html
[7] More info on the SNS can be found at: www.bt.cdc.gov/stockpile/index.asp

- HHS has established eight Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases (RCEs). Each Center is comprised of a consortium of universities and research institutions serving a specific geographical region. The primary objective of the RCEs is to develop and conduct research that supports the development of next-generation medical countermeasures. The RCEs will also be a resource to provide scientific expertise in the event of a biodefense or emerging infectious disease emergency at the national, regional, and local levels.

- At the National Institutes of Health (NIH), funding for biodefense research has increased thirty-fold from 2001 to 2005. These funds support a full spectrum of research aimed at developing new and improved medical tools against potential bioterrorism agents, including vaccines, therapies, and diagnostic tests. NIH already has pursued and surmounted many scientific and technical challenges to quickly move next-generation vaccines for anthrax and smallpox into advanced development, in preparation for the upcoming BioShield procurements of these vaccines. NIH also has gained the interest and support of industry and academia through the awarding of **Biodefense Partnership Challenge Grants** to develop biomedical countermeasures. Research projects include the development of candidate countermeasures for a wide range of biodefense-relevant diseases.

- DoD's U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), the National Institutes of Allergy and Infectious Diseases (NIAID), and DHS have identified 12 new vaccine candidates and a rapid diagnostic system for the highest priority biological threats. Additionally, DoD is deploying an improved **Joint Biological Agent Identification and Diagnosis System**, a system that rapidly identifies biological threat agents.

- The DoD's U.S. Army Medical Research Institute of Chemical Defense (USAMRICD) has developed new preventive treatments designed to be taken before possible exposure to nerve agents. These treatments will be tested in safety clinical trials for eventual use. WRAIR has devised a decontaminating polymer sponge embedded with similar products for cleaning chemical agents from exposed surfaces such as skin.

- In addition to the development of critical medical products, USAMRIID and USAMRICD provide essential training to medical care providers in the

---

"By acting as a willing buyer for the best new medical technologies, the government ensures that our drug stockpile remains safe, effective, and advanced."

President George W. Bush,
July 21, 2004

Medical Management of Chemical and Biological Casualties course. Over 150,000 civilian and military personnel have been trained to date.

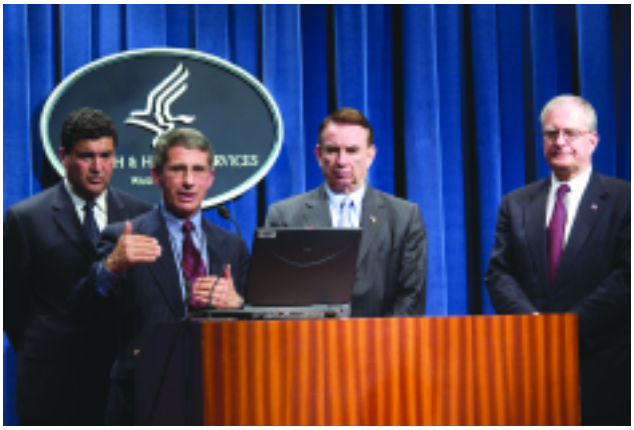
D) Encouraging Research while Ensuring Appropriate Protection against Abuse

The best defense against biothreat agents is the development of vaccines, diagnostics and therapies — work that requires handling, using, and transporting pathogens and toxins. These agents have legitimate medical, commercial, and defensive applications, yet many could be misused to cause serious harm. Many steps have been taken to address the issue of protecting legitimate scientific research while putting into place appropriate safeguards against misuse of this information.

- On March 18, 2005, CDC and USDA's Animal and Plant Health Inspection Service (APHIS) published final rules governing the possession, use, and transfer of select agents (biological agents or toxins deemed a threat to human, animal or plant health).[8] In devising these rules, the Administration has sought to ensure that institutions in possession of select agents provide appropriate physical security, training, and access for individuals with legitimate research needs, while increasing accountability and preventing unauthorized use. CDC and USDA are now in the process of developing final rules, which will make oversight of human, plant, and animal agents and toxins consistent across the Federal government.

- The need for open access to knowledge to promote scientific progress must be balanced against the risk of abuse of dual-use technology. A group of scientific journal editors considered this challenge and issued a statement on February 15, 2003, calling for consideration of processes for effective review of papers that raise security issues.[9] The editors recognized that on occasion, the potential harm of publication might outweigh the potential benefit of publication, requiring that the paper be modified or not be published.

- There is a clear need for expert guidance from the science and security communities to define dual-use research and identify procedures to analyze the risks and benefits associated with dissemination of its results. This need was recognized in particular by the National Research Council (NRC) in its report *Biotechnology in the Age of Terrorism*.[10] On March 11, 2004, the President announced the formation of the **National Science Advisory Board for Biosecurity**.[11] The Board will advise all Federal departments and agencies that conduct or support life sciences research for homeland security, especially dual-use research that could have application to bioterrorism.



HHS Secretary Thompson (third from left) and Zerhouni, Fauci, and Marburger (left to right) announce the creation of the NSABB. Photo credit: HHS photo by Chris Smith

[8] The CDC and APHIS rules governing select agents may be found at: www.aphis.usda.gov/vs/ncie/pdf/btarule.pdf
[9] The Journal Editors' Statement can be found at www.pnas.org/cgi/content/full/100/4/1464
[10] www.nap.edu/books/0309089778/html
[11] www.biosecurityboard.gov

IV. Science and Technology to Counter Terrorism

In addition to developing countermeasures against chemical, biological, radiological and nuclear weapons, the **National Strategy** identified several initiatives where advances in science and technology can be applied to enhance homeland security. The following sections summarize the on-going activities that comprise the foundation of our homeland security S&T efforts.

A) Protecting Agriculture

The agriculture and food industry form a significant segment of the U.S. economy. An attack against this industry would cause economic impacts (direct loss of crops, livestock and assets; lost export markets; significant price fluctuations), environmental concerns, and social and political impacts. Recent naturally occurring outbreaks of Avian Influenza and Exotic Newcastle disease have cost hundreds of millions of dollars to control and eradicate. Since the attacks of 9-11, there has been an increased focus on intentional threats to animal and plant health, as well as to the defense of the food supply beyond traditional food safety efforts. Many programs have been implemented that contribute to our ability to prepare for and respond to natural or intentional introductions of animal or plant disease.

The capabilities of existing laboratories have been increased and additional laboratory capacity has been funded. In addition, coordination among Federal, state, and local laboratories has been formalized. This will enhance our ability to detect and respond to food or agriculture related terrorist incidents.

- The **Food Emergency Response Network (FERN)** [12] is a collaborative laboratory network, co-chaired by the USDA and the FDA that protects citizens by monitoring the food supply for acts of biological, chemical, and radiological terrorism. FERN provides the laboratory capacity to respond to emergencies that is integral to any bioterror surveillance and monitoring system. Two other networks, **FoodNet** [13] (collaborating medical centers that conduct active surveillance for illnesses typically attributable to food-borne pathogens) and **PulseNet** [14] (laboratories that can characterize the unique DNA of food-borne pathogens) allow intensified surveillance and response to outbreaks of gastrointestinal and other potential food-associated disorders, including those outbreaks that might be terrorist-induced.

- The **National Animal Health Laboratory Network** [15], established by the USDA, is a national network of Federal and state diagnostic laboratories that enable a rapid response and surge capacity to animal health emergencies. It is geared to detect and characterize those pathogens that have the potential to be intentionally introduced.

- **The National Plant Diagnostic Network** [16], established by USDA, is a network of regional coordinating labs that focus on enhancing agricultural security by providing detection of and laboratory surge capacity for introduced plant pests and pathogens.

- **The Electronic Laboratory Exchange Network (eLEXNET)** is a secure system that allows multiple government agencies engaged in food

[12] www.crcpd.org/Homeland_Security/Food_Emergency_Response_Network.pdf
[13] FoodNet: www.cdc.gov/foodnet
[14] PulseNet: www.cdc.gov/pulsenet
[15] The National Animal Health Laboratory Network: www.csrees.usda.gov/nea/ag_biosecurity/in_focus/apb_if_healthlab.html
[16] The National Plant Diagnostic Network: www.csrees.usda.gov/nea/pest/in_focus/ipm_if_npdn.html

safety and security activities to compare, communicate, and coordinate laboratory analysis findings. eLEXNET identifies potentially hazardous foods and enables health officials to assess risks and analyze trends. eLEXNET is funded by the FDA and supported by the USDA and DoD.

At the Plum Island Animal Disease Center, the USDA with, support from DHS, is conducting research to improve vaccines to protect livestock against foot and mouth disease (FMD). Current research is focused on demonstrating when animals are fully protected against FMD after vaccination and exploring ways to provide earlier protection using different types of vaccines or producing vaccines with integrated anti-viral activity.

Research is also on-going at other locations. The USDA is conducting research to develop and validate rapid diagnostic tests for agents that may pose a threat to our agricultural system. USDA and FDA are researching rapid tests and sampling strategies to identify threat agents in the food supply and methods to protect food products. FDA is working with Edgewood Arsenal and the Midwest Research Institute for the validation of methods for detecting microbiological agents in foods, and is funding research to evaluate rapid test methods for microbiological analyses of produce samples. In addition, FDA has partnered with DoD to develop and validate methods to detect potential threat agents.

Efforts also are on-going to prepare the country to respond to and recover from a natural or intentional disease incident affecting the agricultural industry.

- **North American FMD Vaccine Bank**. The USDA, in conjunction with Mexico and Canada, maintains a stockpile of vaccines against FMD.
- **National Veterinary Stockpile**. The USDA is developing a stockpile of countermeasures to protect against several animal threat agents.
- **National Plant Disease Recovery System**. The USDA is leading an effort to develop a system of protection and recovery of crops from plant disease threat agents. The system includes research to identify antifungals (substances that will inhibit the growth of or destroy pathogenic plant fungi) to protect crops and to identify crop varieties with resistance to threat agents.

b) 1st Responder Capabilities

As became clear during the events of September 11, 2001, it is imperative that we equip Americans on the front lines of homeland security preparedness and response with technologies and corresponding operational plans that ensure the best possible response to a terrorist event.

With the creation of DHS, we now have a focal point for ideas from the private sector, universities, and other government agencies. DHS maintains close contact with state and local governments to identify the most pressing needs for technologies and technical assistance.

In FY 2004, DHS took steps to boost the ability of Federal, state and local first responders to communicate effectively with one another. **SAFECOM** is a Federal umbrella program under DHS that is dedicated to improving public safety response through the development of standards and a coherent national system that will promote enhanced interoperable wireless communications.

DHS has also initiated the **Regional Technology Integration (RTI) Initiative** to make our cities safer by successfully transferring and integrating existing and advanced homeland security technologies into local governments. This program improves local preparedness and ability to respond to emergencies. The initiative was rolled out in four cities in 2004.

"The first responders of America, all across America, must have the resources necessary to respond to emergencies and save lives."

President George W. Bush,
March 27, 2002

Finally, through the Federal Emergency Management Agency (FEMA), DHS operates a mock hospital facility dedicated to medical training in disaster preparedness and response for hospital and healthcare professionals.

Other Federal agencies contribute with science and technology activities from within their own mission areas that complement the DHS activities and strengthen the Nation's response capability. Some of these are described below:

- NSF and DoD have funded the **Center for Robot Assisted Search and Rescue** at the University of South Florida. The Center has developed robots that assist in the location of survivors in rubble, such as from a collapsed building. The center was involved with rescue efforts at the World Trade Center and, more recently, Hurricane Charlie.

- DoD has established and sustains a training program in medical management of chemical and biological casualties, including training for personnel of the **Theater Army Medical Laboratory (TAML)**, a deployable, modular laboratory that can complete a range of missions including laboratory detection of biological, chemical, nuclear, occupational health and endemic disease threats. Students have included State Department, Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and Secret Service personnel, as well as military services, emergency responders, and officials from select foreign countries.

- To facilitate response and recovery efforts, DHS, DoD and Department of the Interior are working with the government of the District of Columbia to develop a **National Capital Region First Responder Passport Initiative**. This effort, first

Photo credit: Center for Robot-Assisted Search and Rescue at University of South Florida

demonstrated in 2004, will provide a machine readable identity management capability for recognizing first responders.

- **Operation Archangel** is a regional, multi-agency cooperative first responder effort. In Los Angeles, 31 elements of city and county governments have come together to advance homeland security and critical infrastructure protection. The Archangel Team includes participation by the Los Angeles Unified City School District, Los Angeles Fire and Police Department, Public Works, Emergency Management. All core group organizations are acting as a single regional first responder force that facilitates Federal agency interaction and response to needs. DHS and DoD look to Archangel as a test bed for first responder operations testing, evaluation and implementation of hardware and software.

- HHS sponsors research on psychological and behavioral consequences of trauma and chronic threat on children, families, communities, first responders, and the health and human services workforce. The focus of this research is improving stress management and the ability to function under stress, enhancing the Nation's capacity to withstand future critical incidents.

- HHS has funded simulation and modeling research for deploying medical countermeasures. The models assist state and local entities to develop distribution plans for mass protective and preventative treatments, including the staffing, facilities, and training required. A planning guide has been developed to benefit communities.[17]

C) Biometric Identification

Strategies for finding terrorists can be complicated by their efforts to disguise themselves among innocent civilians. As a counter to this, the implementation of biometric technologies (identifying an individual based on physical characteristics, such as fingerprinting, facial recognition, iris scans, etc.) shows great promise in improving the accuracy, consistency, and efficiency of identification devices.

- DHS and State are now using biometric identifiers (a photograph and two digital fingerprints) for visa applicants and travelers to the United States. On January 5, 2004, **US-VISIT**[18] biometric entry procedures were deployed at 115 airports and 14 seaports. US-VISIT is an integrated set of security measures that control the pre-entry, entry, status, and exit of foreign nationals who travel to the

[17] Guide is available at www.ahcpr.gov/research/cbmprophyl/cbmpro.htm

[18] www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml

Biometrics is playing an important role in protecting the United States. These images show the devices used by US-VISIT to capture biometric information from visitors. Photo credit: DHS

United States. NIST tests have shown the US-VISIT fingerprint system to have a 99.5% one-to-one matching accuracy. In its first six months of operation, 559 individuals were identified by biometrics alone as a person on US-VISIT's database. Today, all US visa-issuing posts have begun to capture digital fingerprints and photographs of foreign nationals when they apply for visas, regardless of their country of origin.

- DHS has begun testing several new types of security systems that will involve biometrics: (1) DHS plans to issue 200,000 **Transportation Workers Identification Credentials** to U.S. transportation workers in 2005; (2) the **Airport Access Control Pilot Program** is conducting tests that will include fingerprint or iris recognition to verify the identity of airport employees; (3) five airport sites are evaluating the **TSA (Transportation Security Administration) Registered Traveler Pilot Program**, which uses biometrics to verify the identity of registered travelers who have voluntarily submitted to a background check; and (4) the **TSA Biometric Device Operational Evaluation** has tested nine biometric products, including fingerprints, hand shape, iris recognition, and face recognition systems in a fully operational setting at Knoxville's McGhee Tyson Airport.

- Agencies are working together at the national and international level to develop and implement standards for biometric system interoperability, data interchange, and performance assessments. An Interagency Working Group on Biometrics has been established to coordinate research and development of biometrics technology for homeland security, law enforcement, access control, and intelligence-related applications across the Federal agencies. A collaborative Federal agency effort has already resulted in internationally recognized technology evaluations for facial and fingerprint recognition systems. Also, multiple Federal agencies have recently joined forces in a "Face Recognition Grand Challenge," with the goal to achieve an order of magnitude improvement in the performance of face recognition systems in "real world" environments, which involve changes in pose angle, facial expression, lighting, and background. The group also provides a publicly accessible clearinghouse for research reports, evaluation results, news items, and other biometrics information on the government-sponsored Biometrics Catalog website.[19]

[19] www.biometricscatalog.org

- The FBI is developing its next generation of fingerprint-based identification systems, including improved automated identification, to meet demands for faster responses to fingerprint identification requests.

D) Detecting Hostile Intent

Our ability to prevent a terrorist attack is bolstered by the ability to identify groups or individuals who threaten us. Research in this area includes examination of cultural and sociological factors that may give rise to an environment conducive to terrorism as well as individual biological and behavioral indicators, which may correlate with intent to harm.

- NSF initiated a new five-year research program in human and social dynamics. Emerging research and technological tools provide a window into the human mind that is already revolutionizing the study of human development and cognition, as well as information processing and decision making by groups and individuals. Areas critical to national interests include agents of change, ranging from extremist ideologies to modern technology; the dynamics of human behavior; and decision making and risk, which has special relevance to extreme events.

- In January 2005, DHS announced the selection of the University of Maryland to lead the **Homeland Security Center of Excellence for Behavioral and Social Research on Terrorism and Counter-Terrorism**. The new Center will focus on understanding the nature and extent of the national and international terrorist threat by analyses of the social, cultural, political, ideological, and network property characteristics of terrorists, both as groups and as individuals.

- DHS is supporting research on the detection of deception and criminal intent and on how to maximize screener performance at airports and within other transportation systems so that individuals with intent and capacity to harm can be identified before harm occurs.

- The Intelligence Community and NSF are sponsoring research on the detection of deception that includes investigation and development of behavioral biometrics (measurable behavior traits acquired over time), content analysis in foreign documents and speech, alternatives to the polygraph, and improvements in intelligence analysis by increasing our understanding of thought processes, learning, and decision-making in individuals and teams.

- DoD funds the **Center for Advanced Study of Language** (University of Maryland) to design and implement a research agenda that will help us identify universal verbal (including both spoken and written) and non-verbal (behavioral and auditory) cues in deception.

- Other research supported by DoD involves modeling the underlying memory, attention, and salience processes that are engaged when an individual lies and assessing the usefulness of polygraph signals, saccadic eye movement, cardiovascular changes, and voice stress in the detection of deception.

- The United States Secret Service and the CERT® Coordination Center (CERT/CC) at Carnegie Mellon University, investigated the impact of

threats from "insiders" (trusted personnel) on information systems in critical infrastructure sectors. The study was the first of its kind to provide a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the threats. The findings will help prevent serious crimes such as network intrusions, identity theft, and financial fraud.

E) Coordination of Homeland Security Research and Development

Homeland security is a national challenge, and the science and technology that supports this effort is distributed across the Federal government as well as throughout our country's universities and private sector. Coordination of applicable Federal government research and development occurs primarily through the National Science and Technology Council (NSTC), a Cabinet-level council that advises the President on interagency research programs and priorities. Various other interagency groups also participate in specific coordination efforts. Examples of Federal research and development coordination in homeland security include:

- The White House Office of Science and Technology Policy (OSTP) convened a "blue ribbon" panel on the ***Threat of Biological Terrorism Directed Against Livestock***.[20] This international panel, composed of representatives from Federal, state, and local governments, academia and industry, was tasked with assessing the potential use of biological terrorism directed against agricultural livestock; outlining ideas for the Federal research and development agenda; and prioritizing the steps needed to safeguard industries associated with this sector.

- HHS convened several blue ribbon and expert panels composed of biodefense research experts from across the nation to develop the NIH long-range **Strategic Plan for Biodefense Research**, along with associated national research agendas for medical countermeasures relevant to various categories of pathogens.[21]

F) Laboratory Networks

The National Strategy specified that the DHS should establish a network of laboratories similar to the National Nuclear Security Administration (NNSA) laboratories that provide expertise in nuclear research and development. DHS is taking advantage of the vast research enterprise that already exists and is building upon this foundation to further leverage homeland security research.

- DHS and DOE are partnering to ensure DHS has access to the tremendous resources embodied within DOE's national laboratories and sites. The arrangement elevates homeland security as a primary mission for the laboratories, along with the long-standing national security, energy, and environmental missions.

- DHS has established the **National Biodefense Analysis and Countermeasures Center** (NBACC) at Fort Detrick, Maryland, to study biological

[20] www.ostp.gov/html/STPI.pdf
[21] www2.niaid.nih.gov/Biodefense/Research/strat_plan.htm

agents and provide a world class forensics center, the **National Bioforensic Analysis Center** (BFAC). These centers join other DoD, USDA, and NIH facilities at Fort Detrick to create a **National Interagency Biodefense Campus** that will become a focal point for countermeasures research. Together these agencies will establish research priorities to reduce the threat of biological terrorism, assist in recovery by developing medical treatments, and enhance our ability to identify terrorist perpetrators.

- HHS has awarded funds to build two high containment biosafety level-4 (BSL-4) laboratories and nine regional BSL-3 laboratories around the country. These biocontainment laboratories will provide additional infrastructure for the **Regional Centers of Excellence for Biodefense and Emerging Infections** (RCEs) and other NIAID-funded biodefense research. They will also be available to assist public health efforts in the event of a bioterrorist emergency.

- EPA created the **National Homeland Security Research Center (NHSRC)** which undertakes and supports research and development work on the protection of the country's drinking water supply (including protection, detection, countermeasures, and decontamination); research and development needed for decontamination following a chemical, biological, or radiological terrorist event; and the rapid risk assessment tools needed both by responders and by those who must make longer term "how clean is safe" decisions following any incident.

- The Departments of Commerce, Defense, Energy, Health and Human Services, and Homeland Security, EPA, NRC, and the National Aeronautics and Space Administration (NASA) are organizing the **Interagency Modeling and Atmospheric Analysis Center** (IMAAC) to provide a single point for the coordination and dissemination of atmospheric dispersion modeling and other atmospheric hazard prediction products for incidents of national significance. These predictions will be disseminated to Federal, state, and local responders.

A CDC scientist conducts laboratory research in the Biosafety Level 4 laboratory, Atlanta, GA. Photo credit: CDC

- DHS under the **Cyber Security Testbed Program** has established two multi-university testbed projects with co-funding from NSF. The first of these projects has produced an operational, physical network environment that is similar to, but kept isolated from, the "public" Internet. This network environment will support testing activities (which will continue to be expanded in scale over the coming year). The second project is developing a testing framework and conducting experiments on the physical testbed. These activities are

advancing our ability to conduct simulated attacks, develop an understanding of those attacks, and test cyber security methods and technologies.

G) Technical Analysis

The Federal government regularly seeks technical analysis in matters of science and technology, and is committed to seeking and using the best scientific advice for issues that arise in homeland security. Organizations such as the National Academy of Sciences (NAS) regularly provide expert review and analysis of Government research programs. Already, the NAS has produced a number of reports relating to homeland security that have been helpful to this Administration. Other sources of analysis and advice include:

- In April 2004, DHS announced the establishment of the Homeland Security Institute (HSI) a Federally Funded Research and Development Center that plays a key role in providing critical analysis and decision support regarding security threats, vulnerabilities, and risks. HSI also conducts operational assessments, systems evaluations, technology assessments, and resources and support analyses to help guide S&T priorities and investments.

- DHS is also tapping into the expertise of the academic research community through its university-based Homeland Security Centers of Excellence. To date, four multi-institutional centers have been established: the Homeland Security Center of Excellence for Behavioral and Social Research on Terrorism and Counter-Terrorism led by the University of Maryland; the National Center for Foreign Animal and Zoonotic Disease Defense, led by Texas A&M University; the University Center for Post-harvest Food Protection and Defense, led by the University of Minnesota; the Center for Risk and Economic Analysis, led by the University of Southern California. Proposals are currently being accepted for a DHS Center of Excellence in High Consequence Event Preparedness and Response and are under review for a Homeland Security Cooperative Center of Excellence created by DHS and EPA for the study of microbial risk assessment.

H) Rapid Prototyping and Demonstrations

During Congressional consideration of the Homeland Security Act of 2002, the Administration sought and was granted statutory authority for DHS to use flexible contracting to speed prototype development and field deployment.

DHS has produced an initial version of a fully integrated modeling, simulation, and analysis system for use by government (Federal, state, and local) and industry decision makers to prioritize protection, mitigation, response, and recovery strategies, as well as to support training exercises and provide real-time support during crises and emergencies. The **Critical Infrastructure Protection — Decision Support System (CIP-DSS)** will provide decision support and planning capability across all critical infrastructure sectors, including how these sectors rely on each other. Decision makers will be able to use the CIP-DSS to estimate consequences for individual sectors and assess the potential for cascading consequences across multiple sectors.

In addition, in order to accelerate delivery of promising technologies to first responders, the Administration tasked the interagency Technical Support Working Group (TSWG) to focus on homeland security.

In this role, the TSWG:

- Developed and transitioned chemical protection suits to meet high standards.
- Developed, tested, and transitioned a rehydration system for use with civilian respirator systems.
- Developed and commercialized a kit for training security and response personnel in the recognition of chemical and biological threat agents.
- Developed a working prototype cryptographic module for supervisory control and data acquisition (SCADA) systems. SCADA systems are used with utilities such as natural gas, water, and electric power. The cryptographic module enhances communications protection between network components, protecting against cyber attacks.

With the creation of DHS, further rapid prototyping is being pursued:

- In 2004, DHS completed the first phase of the Counter-Man Portable Air Defense System program designed to adapt military technology to protect commercial airliners from shoulder-fired missiles.
- DHS is working with the U.S. Coast Guard (USCG) to build a prototype integrated maritime surveillance system. This program will integrate existing facilities and upgrade equipment to detect, track and identify vessel traffic in ports, in the zones around them, and over the horizon.[22]
- DHS and DOE are involved in a program to integrate sensors at airports with the operation of ventilation systems, enabling contaminated air to be redirected and allowing time for safe evacuations to occur. Program officials are attempting to develop a comprehensive biological and chemical defense plan that can be used at airports across the country.
- DHS has awarded numerous contracts for technologies that can be rapidly prototyped and deployed to the field. Technologies include CBRN countermeasures; personnel protection; explosives detection; infrastructure protection; physical security; and investigative support and forensics.

- DHS is developing a robust, cost-effective system to protect the DHS mail system, which employs the latest technology and serves as a test bed for new technologies. One of the first technologies considered for testing is the **Autonomous Pathogen Detection System (APDS)**, which detects 11 threat agents and may be expanded to add more agents. The goal is to have a model system that not only meets DHS

[22] www.piersystem.com/external/index.cfm?cid=586&fuseaction=EXTERNAL.docview&documentID=40633

needs but also serves as a model for protection of mail nationwide.

- The National Guard in support of the **Joint Continental U.S. Communications Support Enterprise (JCCSE)** has begun a pilot program to deploy in the field an incident area communications capability. This capability will provide satellite communications, shared situational awareness, and communications networks combining capabilities for domestic response and interoperability with local, state, and Federal agencies. The initial prototypes for this capability have been tested at the Republican National Convention and deployed in support of the Hurricane Ivan relief effort.

- The Department of Transportation (DOT) has established a **24-hour Crisis Management Center** to bring all transportation system incident and response information into one place, with connections to all relevant agencies. DOT is developing quick-response highway and bridge replacement technologies, deploying advanced CBRN and explosives sensors in select transportation systems, and is providing training for dealing with hazardous materials incidents in all modes of transportation.

I) Standards

State and local governments and private citizens need assurance that the systems and equipment they procure will meet all the required levels of safety and efficacy. The Administration is creating mechanisms for analyzing, validating, and setting standards for homeland security equipment. A key element of the President's approach in this area is the participation of the private sector, both to voluntarily adopt certain standards, but also to help create standards of operation and conduct that will protect the Nation.

- DHS adopted four radiation detection standards that establish baseline performance criteria and testing requirements for a number of common types of radiation detectors used by field inspectors and law enforcement officials, ranging from simple radiation pagers (devices indicating the presence of radiation or radioactive materials), to radioisotope identifiers (devices capable of identifying specific materials), and radiation portal monitors (devices designed to screen trucks, freight cars, containers, or other large vehicles).[23] The standards were developed in partnership with NIST, the Department of Energy's National Laboratories, and in conjunction with the Institute for Electrical and Electronics Engineers (IEEE).

- DHS adopted standards for three main categories of CBRN respiratory protection equipment and five standards for protective suits and clothing for responding to CBRN events.[24] These standards have also been adopted by the Interagency Board for Equipment Standardization and Interoperability, which establishes and coordinates local, state, and Federal standardization, interoperability, and responder safety relating to chemical, biological, radiological, nuclear or explosives incident response equipment.

- The Department of Commerce has concluded a two-year investigation of the structural failure and collapse of the World Trade Center buildings to determine necessary changes to building and fire

[23] www.dhs.gov/dhspublic/display?content=3307
[24] www.dhs.gov/dhspublic/display?theme=43&content=3299

codes and standards and practices, as well as plans for how to improve structural and fire analysis methods, emergency response plans, and evacuation procedures. Continued efforts include methods to test high performance building materials and techniques to reduce the vulnerability of buildings to chemical, biological, and radiological aerosols. Studies are also underway to develop tools that improve the movement and communication of people within structures under other emergency situations.[25]

- The NSTC supported an interagency effort to coordinate information on protective action guides (PAGs) following a radiological dispersal device (RDD) or improvised nuclear device (IND) incident. An RDD involves a conventional explosion that spreads radioactive materials over a finite area. An IND is a nuclear device that is assembled by a hostile party, rather than stolen from an existing nation-state's stockpile. Derived largely from existing EPA guidelines, the PAGs were developed to guide the actions of emergency responders in the early and intermediate timeframes following an incident, as well as to assist in defining appropriate long-term cleanup levels.

- NIST is leading an interagency **Internet Engineering Task Force (IETF)** to advance standards and specifications related to internet security (public key infrastructure, network layer security, and key management technologies), as well as other protocols and services that underlie today's Internet. In addition, over the past three years, NIST's Computer Security Division completed over 40 cyber security standards, management, and guidance documents covering a diverse set of cyber security technical areas.

[25] Information about NIST's World Trade Center activities can be found at wtc.nist.gov

[26] www.hsarpabaa.com

J) Cutting Edge Research

The National Strategy recognizes that efforts to secure the Nation will require innovative and revolutionary research and development. The National Strategy directs DHS to establish a program with a high level of programmatic and budgetary flexibility to ensure that high-risk, high-payoff research is conducted.

"To prevail in this war, we will fight on the frontiers of knowledge and discovery."

President George W. Bush,
July 22, 2002

As a primary mechanism for pursuing cutting edge research with the private sector, DHS created the **Homeland Security Advanced Research Projects Agency (HSARPA)** which has issued solicitations and awarded contracts in CBRN detection, cargo container security, automated scene understanding, and bioinformatics.[26]

- DHS established a "virtual" **Cyber Security R&D Center** as the umbrella under which DHS-funded cyber security research and development activities

will be performed. These activities will improve the security of the existing cyber infrastructure and provide a foundation for increased security in the future. Priorities include securing key basic communication protocols on which the Internet relies but which are presently vulnerable to cyber attacks. The next-generation cyber security technology program is focusing current and planned investments on functional needs associated with improving cyber security, including such important areas as secure software development, software assurance, cyber security assessment, wireless security, cyber attack traceback, detection of insider threats, and others. Additional efforts, such as the development of a large-scale testbed network and software testing framework, as well as the creation of large-scale network data sets to support cyber security testing, are aimed at supporting the research and development community and serve to complement the portfolio of investments aimed at functional and infrastructural needs.

Other agencies are likewise pursuing cutting edge research:

- DoD is developing software that can "heal itself" if attacked by detecting and isolating malicious damage and then tracing and undoing the direct and indirect effects. The software will also provide enhanced network security for authentication, data integrity, and privacy.

- NIH has expanded and/or developed several initiatives to provide comprehensive biological agent information to the research community for research to rapidly address the Nation's biodefense needs. Activities include: (1) Microbial Genome Sequencing Centers to meet national needs for genome sequencing, forensic microbial strain identification, and target identification for development of drugs, vaccines, and diagnostics against agents of bioterrorism; (2) Bioinformatics Resource Centers, which will develop and maintain comprehensive relational databases to enable NIH to collect, store, and analyze genomic and related data on deadly pathogens; and (3) a Pathogen Functional Genomics Resource Center, which will provide the research community with the necessary tools to conduct research on disease-causing microbes, including those considered to be potential agents of bioterrorism.

- HHS/NIH has launched several initiatives to engage partners in academia, industry, and other private and public-sector entities to develop biodefense-related diagnostics, therapeutics, and vaccines.

- NSF has over 125 active awards addressing foundational research in cyber security. NSF has created an initiative in **Cyber Trust** with the objective of developing networked systems that are more predictable, more accountable, and less vulnerable to attack and abuse.

Investment in the next generation of homeland security scientists will further advance scientific study in homeland security mission areas:

- DHS has established the highly competitive **Homeland Security Scholars and Fellows Program** to support students and faculty with a commitment to scientific careers in fields that are essential to the homeland security mission. The program provides internships and specialized fellowships for students and faculty to further their

knowledge of homeland security through short- and long-term exchanges at laboratories, facilities, and organizations throughout the homeland security complex.

- HHS/NIH has expanded programs to support training and career development of young scientists in biodefense research. Approximately 30 percent of training grant applications received in FY 2003 were specifically focused on training in biodefense. In addition, an integral component of the NIH-supported Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases program includes training of a new generation of science professionals to perform biodefense research activities.

V. Conclusion

Since the attacks of September 11, 2001, the Administration has led a focused effort to mobilize the Nation's science and technology enterprise to respond to homeland security challenges. We have accomplished much during this time and are looking to the future with new programs and plans to further strengthen the Nation's security. Obviously, much is left to be done.

As long as there are groups and individuals willing to use terror against us, we must continue to maintain a posture of high alert and focus on protecting our citizens. Science and technology is a key foundation in this national effort and one that will continue to make the homeland stronger, safer and better equipped to respond to national emergencies.